Notice of Allowability	**Application No.** 09/905,340	**Applicant(s)** JORDAN, MYLES	
	Examiner Paul Callahan	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment filed 9-29-06*.

2. ☒ The allowed claim(s) is/are *1-3,5-9,13-16 and 18-23*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

   1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.

   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *10/10/06* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

DETAILED ACTION

1. Claims 1-3 and 5-21 were pending in the instant application at the time of the previous Office Action. By virtue of the amendment filed 9-29-06, claims 10, 11, 12, and 17 are cancelled, with new claims 22 and 23 added. Therefore claims 1-3, 5-9, 13-16, and 18-23 remain pending and have been examined.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Justin Stewart on 10/10/06.

3. The application has been amended as follows:

IN THE CLAIMS

Claim 8 is amended to read as follows:

8. A computer program for detecting a computer virus, the program embodied on a computer-readable medium, that when executed causes a computer to:

emulate computer executable code in a subject file;

detect at least one modification to a memory state of a computer system, wherein the at least one modification:

is caused by the emulation of the computer-executable code; and

comprises insertion of a pointer to a viral exception handler, the pointer associated with a particular exception; and

detect at least one instruction, wherein the at least on instruction forces the particular exception.

Claim 9 is amended to read as follows;

9. A computer program for detecting a computer virus, the program embodied on a computer-readable medium, that when executed causes a computer to:

emulate computer executable code in a subject file;

detect at least one modification to a memory state of a computer system, wherein;

the memory state comprises a particular interrupt associated with a legitimate interrupt handler; and

the at least one modification:

is caused by the emulation of the computer executable code;

comprises installation of a viral interrupt handler; and

associates the particular interrupt with the viral interrupt handler instead of the legitimate interrupt handler; and

detect at least one instruction, wherein the at least one instruction forces the particular interrupt.

Allowable Subject Matter

4. Claims 1-3, 5-9, 13-16, and 18-23 are allowed.

5. The following is an examiner's statement of reasons for allowance:

The closest prior art in the field, Nachenberg, does not teach the combination of features of the independent claims, particularly including:

As for claims 1 and 8, the combination of features of the claimed invention, particularly including detecting a modification of a memory state of a computer that is caused by emulation of computer executable code, and comprises insertion of a pointer to a viral exception handler where the pointer is associated with a particular exception. Claims 2, 3, 20 and 21 are dependent from Claim 1 and are thereby allowable on that basis.

As for claims 5, 9, and 16; the novel and unique feature is detection of a modification to a memory state of a computer, where the memory state comprises a particular interrupt associated with a legitimate interrupt handler, the modification is caused by emulation of the executable, and the modification comprises installation of a viral interrupt handler. Claims 6, 7, 22, and 23 are dependent on claim 5 and are thereby allowable on that basis. Claims 18 and 19 are dependent on claim 16 and are thereby allowable on that basis.

As for claim 13, the novel and unique feature is detection of an instruction that forces a particular exception associated with the viral exception handler. Claims 14 and 15 are dependent on Claim 13 and are thereby allowable on that basis.

As for claim 16, the novel and unique feature is detection of an instruction that forces a particular interrupt associated with the viral interrupt handler. Claims 18 and19 are dependent on Claim 16 and are thereby allowable on that basis.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

11-29-06

PEC

Paul Callahan